(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75843 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/15788

(22) International Filing Date: 8 June 2000 (08.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/328,422 9 June 1999 (09.06.1999) US
09/471,127 23 December 1999 (23.12.1999) US

(71) Applicant *(for all designated States except US)*: INTELISHIELD.COM, INC. [US/US]; 10200 W. 44th Avenue, Suite 339, Wheat Ridge, CO 80033 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: FLOYD, Dennis, R. [US/US]; 3265 Fenton Street, Denver, CO 80212 (US). HEATON, Timothy, L. [US/US]; 10875 W. 77th Drive, Arvada, CO 80005 (US). ANDERSON, Stanley, W. [US/US]; 8755 W. 80th Avenue, Arvada, CO 80005 (US). ANDERSON, Brian, S. [US/US]; 8755 W. 80th Avenue, Arvada, CO 80005 (US).

(74) Agent: FOLEY & LARDNER; 777 East Wisconsin Avenue, 33rd Floor, Milwaukee, WI 53202-5367 (US).

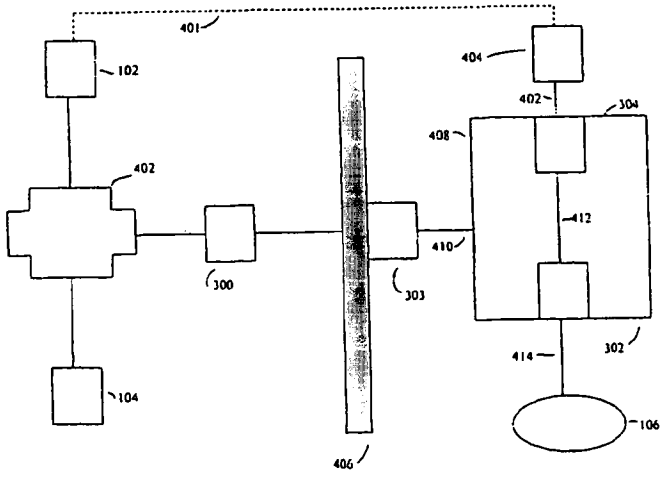
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: INTERNET PAYMENT SYSTEM



(57) Abstract: The present invention is a system and method for providing electronic commerce without providing a buyer's (102) credit card data over the Internet (402), or any other public network. Buyers (102) have a fear of providing their credit card data over the Internet (402). The present invention allows a buyer (102) to make a purchase with their credit card without providing their credit card data over the Internet (402). The present invention provides buyers (102) with a transaction identification number to make Internet purchases and the buyer (102) personally authorizes their purchases while they are on-line. The buyer's (102) actual credit card data is never transmitted over the Internet (402). The on-line affirmation of each purchase through the third party entity that provides the service described by this invention leads to a reduction of fraud.

WO 00/75843 A1

Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Internet Payment System

FIELD OF THE INVENTION

The present invention relates to Internet commerce, also known as electronic commerce. More particularly to credit card purchases over the Internet.

RELATED APPLICATION

This application is a Continuation-In-Part, of Serial Number 09/328,422, filed on 06/09/99, which claims the benefit of U.S. Provisional Application serial number 60/130,121, filed April 20, 1999 and entitled "Internet shopping without transferring credit card data over the Internet".

BACKGROUND OF THE INVENTION

The Internet, world wide web (WWW), is growing rapidly. Electronic commerce has grown substantially year after year. However, buyers still remain wary of making purchases over the Internet for fear of credit card fraud.

Since the Internet is a public network, buyers are fearful of providing their credit card data. Many electronic commerce options are available. None have been able to strike a balance between a system and process that is safe for the buyer, easy for the buyer, alleviates buyer fear, and does not disrupt the current system that sellers currently use.

When a buyer chooses to make a website on-line purchase they may use a credit card. Websites will require the buyer's name, credit card data, expiration date and typically the buyer's address, as well as the address the buyer would like the purchased items shipped to. When providing this data, a buyer types it into their browser, which transmits the data over the Internet, which is a public network. This transmission is not secure, and may be intercepted.

The buyer does not know how secure the server receiving their data is. Even if the transmitted data is not intercepted, someone may still be able to steal the data out of the website's server.

Web sites allow buyers to save their credit card data: actual credit card number, expiration date, name on the card, and other personal information, in the website's database. The next time the buyer shops, their data will be available without the need to type in the data. Once a buyer purchases items at multiple websites, the buyer's credit card data is held by multiple databases on the Internet. Having data in more than one place increases the odds of having data stolen or intercepted.

Secure web-browsers exist, which encrypts the information being sent from the buyers browser to the website server. Typically secure web-browsers use Secure Socket Layer (SSL) technology. Secure servers also exist which utilize encryption, firewalls, and other means in an attempt to save buyers data from being stolen.

However, even with these secure measures the buyer's credit card data is still being sent over the Internet. Servers housing the credit card data, often after it has been decrypted, are accessible, connected to the Internet and, and can be breached by hackers.

An example of current systems and processes is shown in Figure 2, a block diagram illustrating the current e-commerce process and typical credit card transaction process. Figure 2 illustrates a typical credit card transaction process with either a non-Internet seller 200 or an Internet seller 202, in which the process is the same.

Buyer 204 decides to make a purchase with either seller (a non-Internet seller 200 or an Internet seller 202). Buyer 204 then provides their credit card data to either seller, represented by lines 208. Either seller sends the credit card data to standard credit card approval network 206, line 210.

Standard credit card approval network 206 then processes the order and signifies to either seller whether the transaction has been approved or disapproved, line 212. Either seller then informs buyer 204 whether the transaction has been approved or disapproved, line 214.

Current systems allow either seller to view buyer's 204 credit card data. The Internet seller, through interaction with buyer 204, also receives the data, line 208, over a public network, the Internet.

Other options exist, two patents are discussed below.

U.S. Patent No. 5,826,241 ('241) discloses a computerized system for making payments and authenticating transactions over the Internet. The '241 patent requires both the buyer and the seller to have an account with the system. The '241 invention inserts itself into each financial transaction, charges the buyer's credit card, receives payment from the company the buyer has a credit card seller account with, may remove credit card fees and service charges, and then passes the money onto the seller. The seller is paid long after the purchase is consummated, maybe 30 days or more. Electronic mail (E-mail) is used to verify a purchase with a buyer, which may be a time consuming process. Transactions are approved by the buyer via email utilizing either "yes", "no", or "fraud" in the E-mail messages. The '214 patent uses the buyers' surrogate credit card number as the personal identification number (PIN) and shares the surrogate credit card number with the seller.

U.S. Patent No. 5,757,917 ('917) discloses a computerized payment system for purchasing goods and services on the Internet. Transactions are approved by the buyer via E-mail utilizing either "yes", "no", or "fraud" messages, which are slow and time-consuming. The '917 patent uses the buyers' surrogate credit card number as the personal identification number (PIN) and shares the surrogate credit card number with the seller. The '917 patent also uses hardwired ethernet connections between an Internet-connected computer, "front end" and a computer, "back end", which contains both the surrogate and actual credit card data and which communicates with the credit card approval network.

Buyers are wary of how their data is transmitted, who has access to the data, where the data is being stored, how long the data is being stored, and how secure the server storing the data is.

A need exists for storing buyers' credit card data securely and keeping the data from ever being transmitted over a public network such as the Internet.

There is a need to facilitate electronic commerce credit card transactions in a secure and time-efficient manner without changing the current credit card seller account systems that presently exist. A standard credit card processing method exists and is currently used by every seller who accepts credit cards. A system that requires sellers to acquire new

accounts or to otherwise alter their standard order processing system may not be cost effective or may be unacceptable to sellers.

Sellers may not want to sign up for another service, apply for the service, go through the typical credit and background checks, which result in the need to set up additional accounting procedures, and receive yet another monthly statement and invoice. Sellers need a system that alleviates buyer fears and requires no additional hardware, software, or other costly and time consuming procedures to implement.

A need exists for buyers, who decide to make a purchase to securely make purchases over the Internet with as little effort and disruption as possible for either the buyer or the seller, without abandoning the present credit card processing method.

Until the present invention, the foregoing needs and problems had not been met or solved.

FEATURES AND ADVANTAGES

The present invention has multiple features and advantages, a few of which are discussed below, others will be apparent from the entire disclosure.

The present invention eliminates buyer fears about releasing credit card data. Buyers' credit card data is kept securely and never transmitted over a public network such as the Internet.

With the present invention it is not necessary for sellers to purchase additional hardware, nor software. The code that controls the sellers' Internet order forms is simply modified by the provider of the service described in this invention. The seller participates if so desired.

When using the present invention, as far as the seller is concerned, the standard credit card transaction takes place and the seller receives their payment through their seller account provider just as with any other of their credit card transactions.

A seller does not need a secure site, digital identification certificate, and other time consuming and expensive additions to their web site for the purpose of providing secure transmissions for Internet commerce when using the present invention. Credit card data is never sent over a public network, such as the Internet.

The present invention provides the buyer with the service of completing the seller's order form and including in the credit card data field a unique transaction identification number (TIN) that is unique, being generated for each purchase by the provider of the service described herein (the "Provider"). The buyer sends this completed form to the seller to authorize the transaction and the seller records the TIN and forwards the TIN to the normal credit card approval network (CCAN) in the same manner as any other electronic purchase. The TIN includes the Provider's bank identification number (BIN) which alerts the CCAN to contact the Provider over dedicated secure data transmission lines (not the Internet) to obtain the buyer's actual credit (or debit) card data by presenting the TIN unique to this purchase. This card data is then passed through the normal CCAN and an approval/decline notice is sent to the seller by the CCAN.

Due to the present invention, wherein a third party confirms each online purchase, sellers may be the victims of less fraud.

The buyer needs to open and maintain an account with the Provider. A buyer receives an account number and selects a personal identification number (PIN). Neither the credit (or debit) card data, nor the account number, nor the PIN is ever revealed to the seller to make a purchase using the present invention.

The buyer's credit card data is kept on a secure server and is never transmitted over the Internet to make a purchase when using the present invention.

Buyers personally enter their credit card data into the secure server during the initial enrollment process, either by using a 1-800 number and talking with a customer service representative of the Provider or on line at the Provider's web site. Buyers may enter credit (or debit) card data for multiple cards which may allow the buyer the flexibility of choosing which card to use to make a purchase.

The buyer invokes the present invention by clicking an icon that has been placed on the buyer's personal computer by the Provider during subscription or, when using a different computer, by contacting the Provider's web site. The invocation of the present invention is done instantly and in real-time.

The buyers' credit card data is kept on a server located behind a firewall, and multiple other security barriers.

Working in conjunction with enhanced networking security protocols, the server also utilizes advanced multi-layered data mining and data management application programming interfaces to protect the internal data structures from data access outside of the standard transaction process. Additionally, the server utilizes multiple data filters to prevent data outflows from transmission pathways other than those included in the transaction process.

Extensive software does not need to be loaded onto the buyer's computer. The buyer may use any internet connected computer, anywhere, without the need for installing extensive software. The Provider merely downloads 4 lines of html code that establishes the Provider's icon on the buyer's computer.

The present invention also checks the buyer's preferred shipping address with the address(es) provided by the buyer at the time of purchase. This check provides yet another level of security. If a credit card is lost, a criminal could order merchandise and have it shipped to the criminal's account. If the account number is lost, the criminal must also know the PIN number to be able to purchase merchandise with the account. Even if the PIN number is lost, the merchandise will only be shipped to the address(es) contained on the secure server. The criminal will not be able to send the merchandise to an address of the criminal's choosing without entering additional information which is other than the account number or the PIN number, such as a portion of the person's social security number or the name of a relative, i.e. data that would not be known to the criminal.

Another level of buyer security comes from the fact that the buyer's credit data is only on one server, not spread throughout the Internet on multiple seller servers.

Therefore, the buyer may inactivate their account by only having to access only one server, which denies use of the buyer's credit card data by everyone.

A buyer is able to validate their purchase in real time while on-line. A transaction only occurs after correct verification of the account number, PIN, and shipping address.

SUMMARY OF THE INVENTION

The present invention is a system and method for providing electronic commerce without providing a buyer's credit card data over the Internet, or any other public network. The buyer uses a surrogate credit card number to make purchases over the Internet. A different surrogate number is used for every purchase, thus impeding the ability of sellers to track a buyer's buying habits. An ultra-secure server network is provided in which the surrogate credit card number can only be translated into the actual credit card data when the buyer, who is on-line while a purchase is being made, personally authorizes the purchase using a separate personal identification number. The converted credit card data is transmitted directly to the bank that handles the seller's credit card account, just as though the buyer's actual credit card were physically passed through a point-of-sale terminal at the seller's premises. The data then proceeds through the standard electronic credit card approval network. The surrogate card issuer acts as a front-end, independent third party enabling prior buyer approval of each transaction while operating seamlessly with the standard credit card approval system.

BRIEF DESCRIPTIONS OF THE DRAWINGS

A more complete appreciation of the invention and many of the attendant advantages thereof will become better understood when referring to the accompanying drawings wherein:

Figure 1 is a block diagram illustrating the process of the present invention.

Figure 2 is a block diagram illustrating the current e-commerce process and standard credit card transaction process.

Figure 3 is a block diagram illustrating the process of the present invention as shown in Figure 1, in more detail.

Figure 4 is a block diagram illustrating the overall process of the present invention between servers.

Figure 5 is a block diagram of the transaction process for the present invention.

Figure 6 is a block diagram continuing the transaction process of Figure 5 for the present invention.

Figure 7 shows a continuation of the purchase transaction process.

Figure 8 is a block diagram illustrating a step from Figure 7 with additional steps.

Figure 9 is a block diagram of the process for establishing a buyer's account with the present invention.

Figure 10 is a block diagram of the process for establishing a seller's membership with the service that implements the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to the figures, figure 1 is a block diagram illustrating the process of the present invention. The present invention internal network 100 is illustrated by block 100. Buyer 102 interacts with seller 104. Transactions are made through a standard credit card approval network 106.

Lines labeled 108 through 122 illustrate the process of the present invention. Line 108 illustrates buyer 102 choosing to purchase a product or service and utilize internal network 100. Buyer 102 sends the following to internal network 100: seller ID, transaction amount and the Internet protocol address of buyer 102, line 110. Internal network 100 activates a new two-way browser session with buyer 102, represented by line 112, by utilizing the internet protocol address supplied by mercbuyer 102.

The browser screen displayed on buyer's 102 monitor details to buyer 102 seller's 104 name and transaction amount and prompts buyer 102 to enter their account number and PIN to verify their identity. Buyer 102 sends this data to internal network 100, still using the two-way browser session, line 112.

Internal network 100 verifies that buyer 102 has a valid account with Provider and invites buyer to select a credit (or debit) card and shipping address, again using browser session line 112. Buyer responds with choices, line 112.

Internal network 100 then closes the browser session and activates a Transaction Processing Application which uses electronic commerce modeling language (ECML) or similar open protocol, to complete the seller's 104 order form; generate a unique transaction identification number (TIN); place the TIN in the credit card data field of seller's form; and place this completed form on the buyer's 102 monitor, line 114. Buyer 102 then approves the purchase by clicking "approve" on the monitor, which sends the completed form to the seller 104, line 116.

Seller 104 records the TIN and forwards it to the normal credit card approval network (CCAN) 106, line 118. The Bank Identification Number (BIN #) found within each TIN notifies the CCAN to contact Internal network 100 and present this TIN to obtain the actual credit card data, line 120. The Internal network 100 checks the validity of the TIN and provides the corresponding buyer's 102 actual credit (or debit) card data to the CCAN, line 122.

The CCAN then processes the transaction in the normal manner, sending an approval or decline notice to seller 104, line 124. Seller 104 notifies buyer 102 of the results of the transaction, line 126. Seller 104 never receives or views the buyer's 102 account number, PIN or actual credit (or debit) card data to make this transaction.

The transaction is now complete, buyer 102 has made a purchase, seller 104 has made a sale, and standard credit card approval network 106 has processed the credit card transaction. Neither seller 104 nor standard credit card approval network 106 have seen or

done anything different than they do with a normal credit card transaction once the surrogate number is replaced by the actual card number.

Figure 3 is a block diagram illustrating the process of the present invention as shown in Figure 1, in more detail.

Blocks and lines, 100 through 126 are identical to Figure 1. Please read Figure 1 in conjunction with Figure 3. The following information describes the present invention internal network 100 in greater detail.

Internal network 100 consists of web server 300 which is connected to the Internet. Web server 300 registers buyers and receives transaction data from merchant buyer 102, including: seller identity, and Internet Protocol (IP) address for this on-line session of buyer 102 who desires to make a purchase of goods and/or services from seller 104, line 110. Web server 300 then activates a two-way browser session with buyer 102 monitor, represented by line 112.

Provider, who operates internal network 100, prompts buyer 102 to enter their account number and PIN, line 112. Buyer 102 enters and sends this data to web server 300, line 112. Web server 300 transmits the data to database server 303, line 306.

Server 303 is part of a network operated behind a secure firewall by the entity that provides the service described in this invention.

Server 303 compares the account number and PIN for validation and, line 308, transmits, via web server 300 and browser session, line 112, with buyer 102, a request for which pre-stored credit (or debit) card and shipping address to use for this purchase. Buyer provides this data via browser session, line 112, to web server 300 and on to data base 303, line 310. This also activates the transaction process application (TPA) in application server 304. The TPA sends this information along with the TIN to the Web Server which then completes the sellers order form and generates a unique transaction identification number (TIN) and inserts the TIN into the field in the form reserved for the credit card data. The completed form is passed to web server 303, line 312, and on to buyer 102, line 114.

Buyer 102 then authorizes the purchase by sending the completed form to the seller 104, line 116. Seller 104 records the TIN and transmits it to the credit card approval network (CCAN) just as is done with any other credit card purchase, line 118. The CCAN recognizes, from information contained in the TIN, the need to visit internal network 100 to obtain the actual credit card data that will be used to process this transaction. This is done by routing the TIN to authorized processor 302, line 120. Authorized processor 302, is pre-authorized by Provider to use dedicated, secure (non-Internet) telecommunication links to enter internal network 100, line 314. The TPA compares the TIN to that generated in line 310 and if valid, provides the actual credit (or debit) card data that corresponds to this unique transaction to the authorized processor, line 316.

Authorized processor 302 transmits the actual card data to the CCAN, line 122. The CCAN now processes the card data in the manner normal for any transaction and transmits an approval/decline notice to seller 104, line 124. Seller 104 notifies buyer 102 of the result, line 126.

The transaction is now complete, buyer 102 has made a purchase, seller 104 has made a sale, and standard credit card approval network 106 has processed the credit card transaction. Neither seller 104 nor standard credit card approval network 106 have seen or done anything different than they do during normal credit card transactions. The TIN is used by the authorized processor to identify the transaction and settle any post-transaction activities such as disputes, charge-backs, credits, exchanges, etc.

Figure 4 is a block diagram illustrating the overall process of the present invention between servers. Shown in Figure 4 are the pathways between the various servers, layers of security represented by the firewall, and the gateways. Buyer 102 and seller 104 are connected to Internet 402. Web server 300 is connected to Internet 402 and to server 303 and server 304 through security firewall 406 and gateway 410.

Buyer Call Center 404 is accessed by buyer 102 through conventional phone lines, line 401, to a specific phone at the number listed in buyers 102 subscription.

Buyer 102 provides their actual credit (or debit) card data and preferred shipping address(es) either on line through web server 300 and gateway 410 into database server 303

or by phone to a customer service representative who enters this data through gateway 402 into database server 303. Server 303 and transaction processing application server 304 are in close proximity within a highly secure area with restricted access, both physical and electronic.

Authorized processor 302 is connected to standard credit card approval network 106 through dedicated communication line 414 and also accesses server 304 via gateway 412, completing the system. Seller 104 is connected to the credit card approval network 106 via dedicated communication line 416, not the Internet.

Figure 5 is a block diagram of the transaction process for the present invention. In step 500 the buyer decides to make a purchase at a seller's website. In step 502 the buyer proceeds to checkout, to pay for the products or services selected.

In step 504, the buyer selects to use the present invention as their payment vehicle. Selecting the present invention is as simple as clicking on an icon or text link which signifies the present invention and is recognized by the buyer.

The action of step 504 causes the the current IP address of the buyer to be sent along with the transaction amount and the seller account ID to the web site of the present invention, step 506. In step 508, the web site activates a two-way browser session with buyer, identifies the transaction, amount and seller, and requests buyer's account ID number and PIN. These steps are transparent to the seller and the seller does not know what is going on between the present invention's web site and the buyer.

Figure 6 is a block diagram continuing the transaction process for the present invention. Step 610 prompts the buyer for account ID and PIN.

In step 612 web server queries the secure intranet server operated by the Provider for validation of the buyer account ID, and PIN. Step 614 determines if the data is valid and requests from buyer which credit card and shipping address to use for this transaction, step 618. This shipping address is checked against those previously entered by the buyer, step 620. If a different shipping address from one stored is selected, then additional verification of buyer's identity is requested, step 622. This information is compared to

information entered by buyer during enrollment, step 624. If not valid, a failure notice is sent to both buyer and seller, step 628.

If valid, the browser session is closed, and the transaction processing application (TPA) is initiated and appears on the buyer's monitor, step 626. Provider creates a single-use transaction identification number (TIN), places TIN in the data field used for credit card data on the seller's order form and completes the remainder of the form using data previously provided by the buyer.

The buyer verifies the accuracy of the form as it appears on his or her monitor, step 630. If inaccurate, buyer is advised to contact customer services and transaction is canceled, step 632. If accurate, buyer is asked to authorize the transaction, step 634. If the buyer does not authorize the transaction, it is canceled and the seller is so notified, step 636. If the buyer approves the transaction, the completed form is transmitted over the Internet to the seller, step 638.

Figure 7 shows a continuation of the purchase transaction process. The seller processes the transaction as any other, sending the TIN to the normal credit card approval network (CCAN) used by the seller for electronic commerce transactions, step 712. The CCAN tests the bank identification number (BIN) present within all credit card numbers to determine routing path, step 714. If the BIN unique to the Provider of the service described in the present invention is not present in the TIN, it is routed through the normal CCAN transaction approval process, step 722.

If the Provider's BIN is present, it is routed to the Provider's internal network to obtain the actual credit card number, step 716. The TIN is checked by the Provider's TPA, step 718. If the TIN is valid, the actual card data is provided to the CCAN, step 720, and is then routed through the normal credit approval process, step 722. If the TIN is not valid, the transaction is terminated and the CCAN is notified by the Provider, step 724. The seller is notified in the normal manner by the CCAN whether the transaction is terminated, approved or declined, step 726. The seller then notifies the buyer of the transaction status, step 728.

PCT/US00/15788

mer service representative who enters this data through gateway 402)3. Server 303 and transaction processing application server 304 are :hin a highly secure area with restricted access, both physical and

:essor 302 is connected to standard credit card approval network 106 imunication line 414 and also accesses server 304 via gateway 412, Seller 104 is connected to the credit card approval network 106 via on line 416, not the Internet.

ock diagram of the transaction process for the present invention. In ides to make a purchase at a seller's website. In step 502 the buyer :o pay for the products or services selected.

: buyer selects to use the present invention as their payment vehicle. invention is as simple as clicking on an icon or text link which vention and is recognized by the buyer.

;tep 504 causes the the current IP address of the buyer to be sent :ion amount and the seller account ID to the web site of the present In step 508, the web site activates a two-way browser session with transaction, amount and seller, and requests buyer's account ID ese steps are transparent to the seller and the seller does not know :en the present invention's web site and the buyer.

block diagram continuing the transaction process for the present ompts the buyer for account ID and PIN.

b server queries the secure intranet server operated by the Provider uyer account ID, and PIN. Step 614 determines if the data is valid :r which credit card and shipping address to use for this transaction, ig address is checked against those previously entered by the buyer, ent shipping address from one stored is selected, then additional identity is requested, step 622. This information is compared to

). The CCAN has seen a nded in their normal fashion. in a fully secure manner with y have completed a purchase ssurance that the transaction provide complete privacy of

account with the Provider of 's web site and activates the ard enrollment information, :cts a personal identification ithentication as well as an he buyer, step 814.

subscription agreement, step 18. If the buyer agrees, the over this encrypted Internet ng, buyer is invited to enroll ntative of Provider, step 822. :count number and a phone /e to complete the application

:hat session, the data will be erified by Provider over the not valid, the buyer will be is provided, step 830. If the d in Figure 9. The Provider uses this account number and e, step 912. Buyer views the service and views the Seller

Yellow Pages to determine which sellers allow purchases using this secure service, step 914.

The buyer is asked if they now want to activate their account with the service so it can be used to make purchases, step 916. If the buyer does not want to make purchases immediately, their account will remain inactive until they choose to activate it, step 918. If the buyer is ready to make purchases, the account is activated and can be used to make purchases at any time, step 920. Once purchasing activity has been completed, buyer will be asked whether the account should remain active, step 922. If the buyer answers "yes", the account will be available to purchase whenever the buyer shops at a seller certified to use this purchasing system, step 920. If the buyer answers "no", the account will be placed on an inactive status, step 918. In this status, no one can use the buyer's stored credit (or debit) card(s) to make purchases and only the member can activate the account.

While the present invention does not require that a Seller establish an account with the Provider, some sellers may elect to do so as an added convenience and security measure for their customers. In such event, Figure 10 is a block diagram of the process for establishing a seller's membership with the entity providing the service described in the present invention. In step 1002 a seller requests to be registered with the system.

Step 1004 then attempts to determine if the seller is qualified to be registered by meeting the following criteria: currently accept, at minimum, Visa and/or MasterCard (either credit or debit); currently has an e-commerce web presence and has been conducting e-commerce for approximately one year; their defined e-commerce methodology is compatible with the present invention; their e-commerce platform meets the system requirements of the present invention; they meet credit worthiness requirements and are a business in good standing, presumably accomplished through the Dun & Bradstreet directory.

If the seller is not approved, then the process ends. Upon approval the process passes to step 1006 in which an agreement is executed.

In step 1008 the seller provides the following data: credit card seller processor seller identification number, seller processor name, appropriate contact data at the seller

processor. The present invention then contacts the seller processor and provides the seller processor with the Bank Identification Number (BIN) that will be found in the TIN, and directions for routing the TIN to the present invention to obtain the actual credit card number.

Step 1010 then assigns the seller a member-seller identification and creates a record for the seller within the present invention terminal server. This record includes the following: Seller ID, seller name and contact data, processor name and contact data, processor seller ID, and telephone number for transaction processing.

In step 1012 the present invention then provides a few lines of HTML code to the seller that the seller can "cut and paste" into the seller's existing platform to offer the present invention as another payment option path to buyers. Embedded within this code is the ability to transfer the total transaction purchase price and the seller's account. Upon testing, verification, and certification, the seller is set up and may begin accepting transactions.

In another embodiment, the surrogate credit card number and/or PIN does not have to be a number, it may be a digital certificate or other means of identifying the buyer.

Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

CLAIMS

What is claimed is:

1. A method for allowing buyers to make private and secure real-time electronic commerce purchases using credit or debit cards without providing the buyer actual credit card data to the seller or over a public network, comprising the steps of:

receiving a purchase request from a buyer or a seller;

receiving a buyers' account identification number from the buyer;

receiving the buyers' personal identification from the buyer;

generating a transaction identification number that is unique to this specific transaction;

transmitting the transaction identification number to the buyer;

buyer authorizing the purchase by transmitting the transaction identification number to the seller;

seller processing the transaction by sending the transaction identification number to the seller's credit/debit card processor for routing through the normal approval network for credit, or debit, card transactions, and

transmitting the buyers' credit card data to a Provider-authorized processor operating within the normal credit card authorization network upon verification that the received transaction identification number matches the unique transaction identification number generated for this transaction.

2. The method for facilitating secure electronic commerce as in claim 1, further comprising the step of:

transmitting a purchase authorization screen to the buyer.

3. The method for facilitating secure electronic commerce as in claim 2, further comprising the step of:

determining the internet protocol address of the buyer for the transmission of the purchase authorization screen.

4. The method for facilitating secure electronic commerce as in claim 2, further comprising the step of:

displaying a purchase authorization screen to the buyer for the purpose of obtaining the buyers' account identification and personal identification number.

5. The method for facilitating secure electronic commerce as in claim 1, wherein an order request from a seller comprises: a sellers' ID, a transaction amount.

6. The method for facilitating secure electronic commerce as in claim 5 wherein a two way browser session is established between a buyer and a provider of the method.

7. The method for facilitating secure electronic commerce as in claim 5 wherein an order request from a buyer or a seller further comprises an internet protocol address of the buyer.

8. The method for facilitating secure electronic commerce as in claim 1, wherein receiving the buyers' account identification and receiving the buyers' personal identification number comprises receiving the account identification and personal identification number directly from the buyer without ever revealing the account identification or the personal identification number to the seller.

9. The method for facilitating secure electronic commerce as in claim 8, wherein a transaction identification number includes a bank identification number that informs a seller processor where to route the transaction to retrieve an actual credit card number to process for this transaction.

10. The method for facilitating secure electronic commerce as in claim 9, wherein a buyers' personal identification is a number.

11. The method for facilitating secure electronic commerce as in claim 6, further comprising the step of:

comparing the buyers' shipping address with the shipping address provided by the buyer at the time of enrollment.

12. The method for facilitating secure electronic commerce as in claim 14, further comprising the steps of:

upon determining the buyers' shipping address is different than the shipping address provided by the buyer:

requesting another form of identification from the customer to verify the customer would like to have their purchase shipped to the new shipping address.

13. A method for facilitating secure electronic commerce without providing a buyers credit card data over a public network in real time, comprising the steps of:

receiving an order request from a seller or a buyer containing an internet protocol address of a buyer, a seller ID;

displaying a purchase authorization screen to the customer in a two way browser session between buyer and provider of the method at the internet protocol address sent by the seller;

receiving a buyers' transaction identification number and personal identification number from the buyer through the purchase authorization screen;

comparing buyers' transaction identification number the transaction identification number generated by the internal network, and

upon successful comparison, providing the buyers' credit card data to the sellers' seller account processor.

14. The method for facilitating secure electronic commerce as in claim 1, further comprising the steps of:

receiving the buyer's credit card data, and

maintaining the buyer's credit card data on a secure server which is not connected to a public network.

15. A system for facilitating secure electronic commerce without providing a buyers credit card data over a public network in real time, comprising:

a first computer containing buyer credit or debit card data, and

a second computer connected to said first computer containing a transaction processing application program.

16. The system for facilitating secure electronic commerce as in claim 15, further comprising:

a third computer connected to the internet containing a program for communicating with sellers and communicating with buyers, and

a seller processor securely connected to said second computer for relaying communications from said second computer to said first computer.

17. The system for facilitating secure electronic commerce as in claim 15, further comprising:

an on-line system wherein said first computer contains a program allowing the buyer to enter their credit card data through said on-line network through a secure gateway into said first computer.

18. The system for facilitating secure electronic commerce as in claim 16, further comprising:

a Provider-authorized processor that is also part of the normal credit card approval network connected to said second computer containing a program for processing credit card transactions.

19. The system for facilitating secure electronic commerce as in claim 16, wherein the security between said seller processor and said third computer is a firewall.

20. The system for facilitating secure electronic commerce as in claim 15,

wherein said first computer contains a program for converting buyer surrogate credit card data into actual buyer credit card data.

21. The system for facilitating secure electronic commerce as in claim 15,

wherein said first computer contains a program for securely receiving buyer credit card data over the internet.

22. The system for facilitating secure electronic commerce as in claim 16, wherein the connection between said first computer and said fourth computer is wireless.

23. The system for facilitating secure electronic commerce as in claim 15, wherein the connection between said first computer and said second computer is wireless.

24. The system for facilitating secure electronic commerce as in claim 16, wherein the connection between said third computer and said fourth computer is wireless.

25. The system for facilitating secure electronic commerce as in claim 15, wherein said first computer is securely connected to the internal network.

26. Computer executable software code stored on a computer readable medium, the code for facilitating secure electronic commerce without providing a buyers credit card data over a public network in real time, comprising:

code for initiating a browser session on a buyers computer containing data regarding a purchase,

code for receiving the buyers identification, and

code for transmitting buyers identification.

27. Computer executable software code stored on a computer readable medium as in claim 26, further comprising:

code for approving the buyers identification, and

code for completing a credit card transaction upon approval of buyers identification.

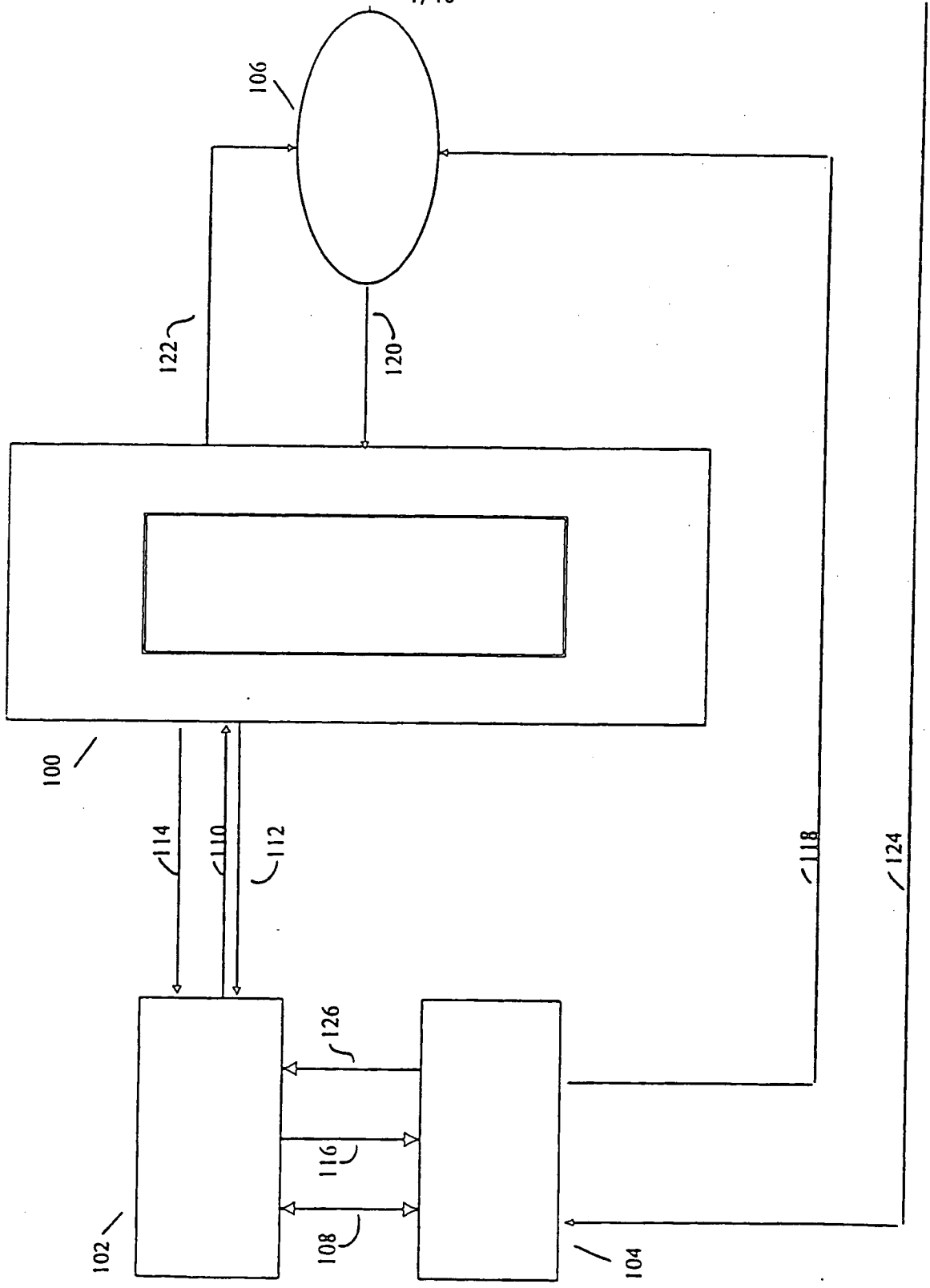


FIGURE 1

PCT/US00/15788

ıtable software code stored on a computer readable medium
;ing:

ing the buyers identification, and

ıleting a credit card transaction upon approval of buyers

FIGURE 2

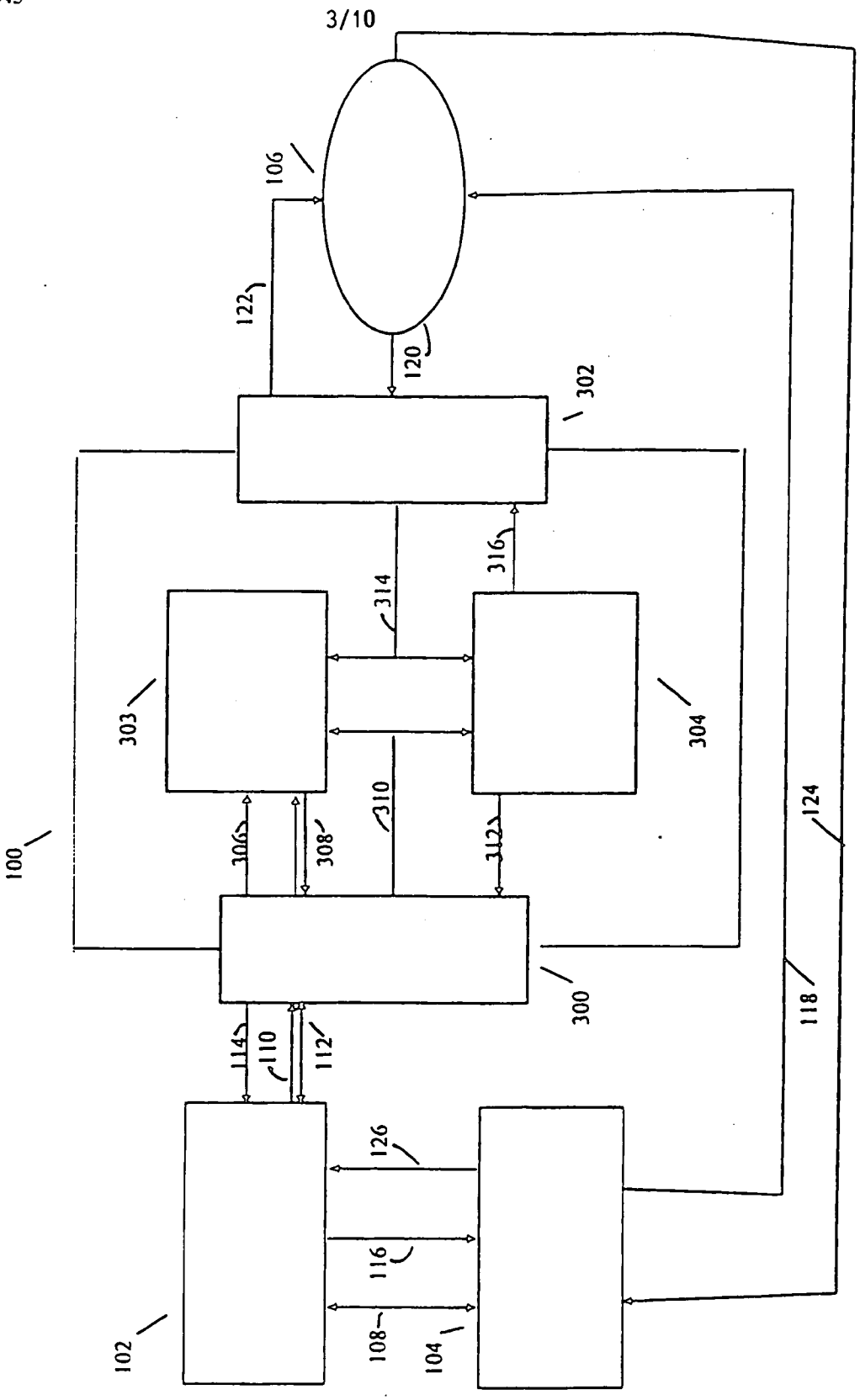


FIGURE 3

PCT/US00/15788

:utable software code stored on a computer readable medium
sing:

/ing the buyers identification, and

)leting a credit card transaction upon approval of buyers

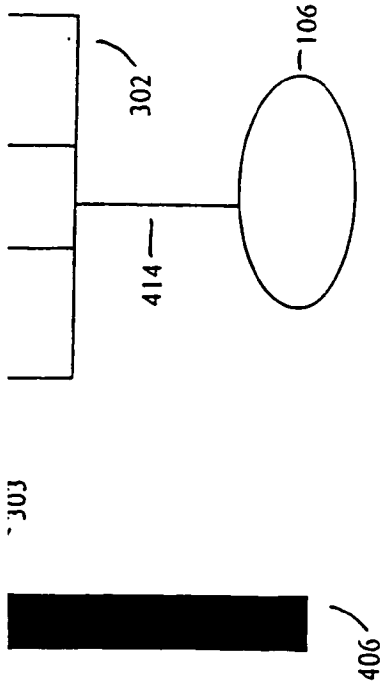


FIGURE 4

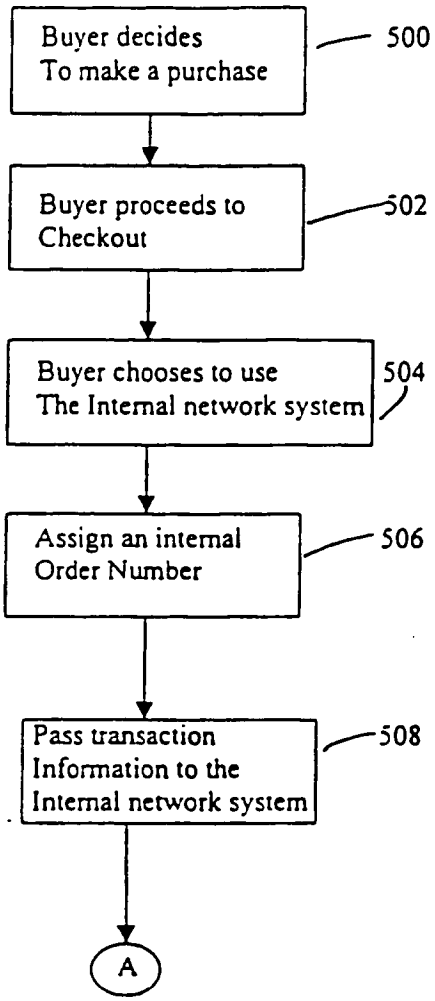


FIGURE 5

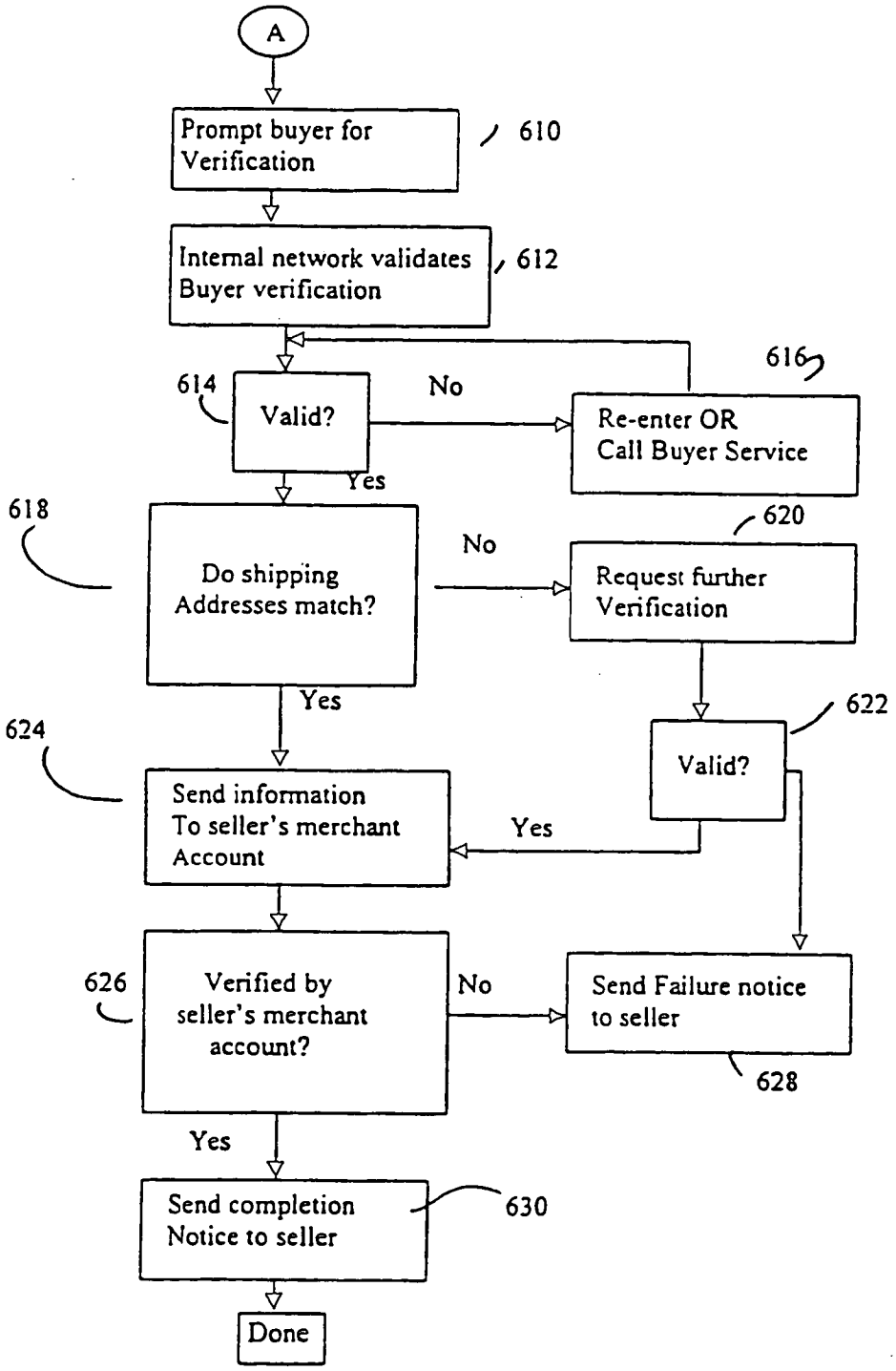


FIGURE 6

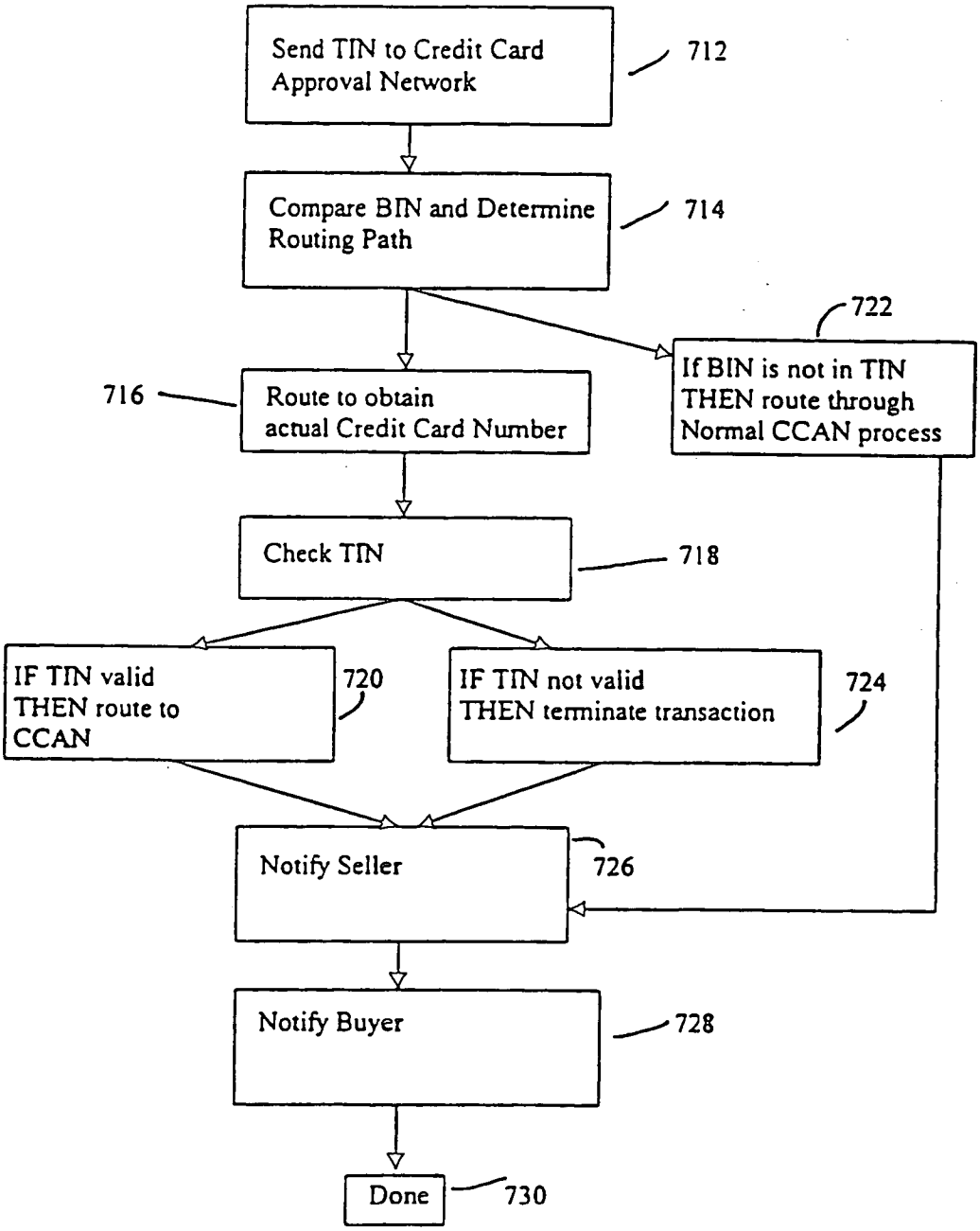


FIGURE 7

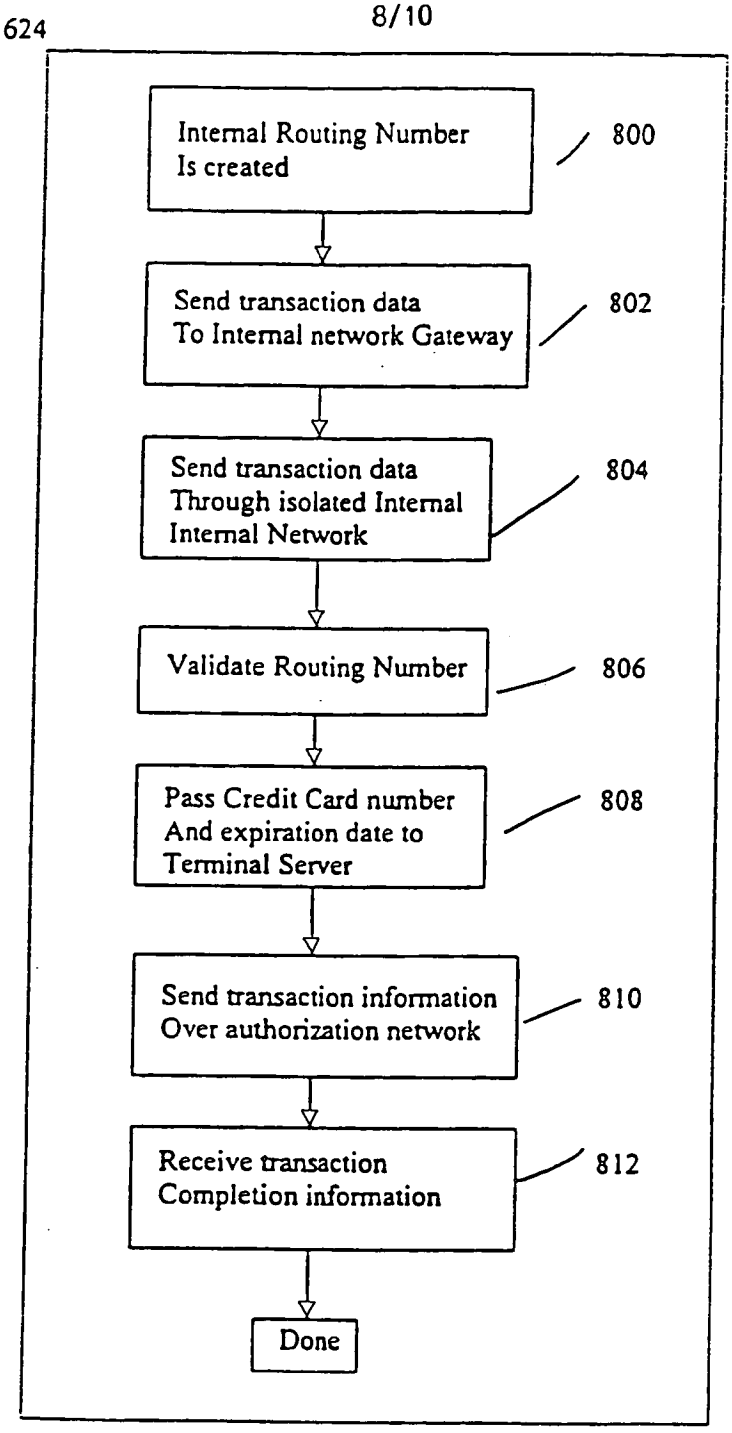


FIGURE 8

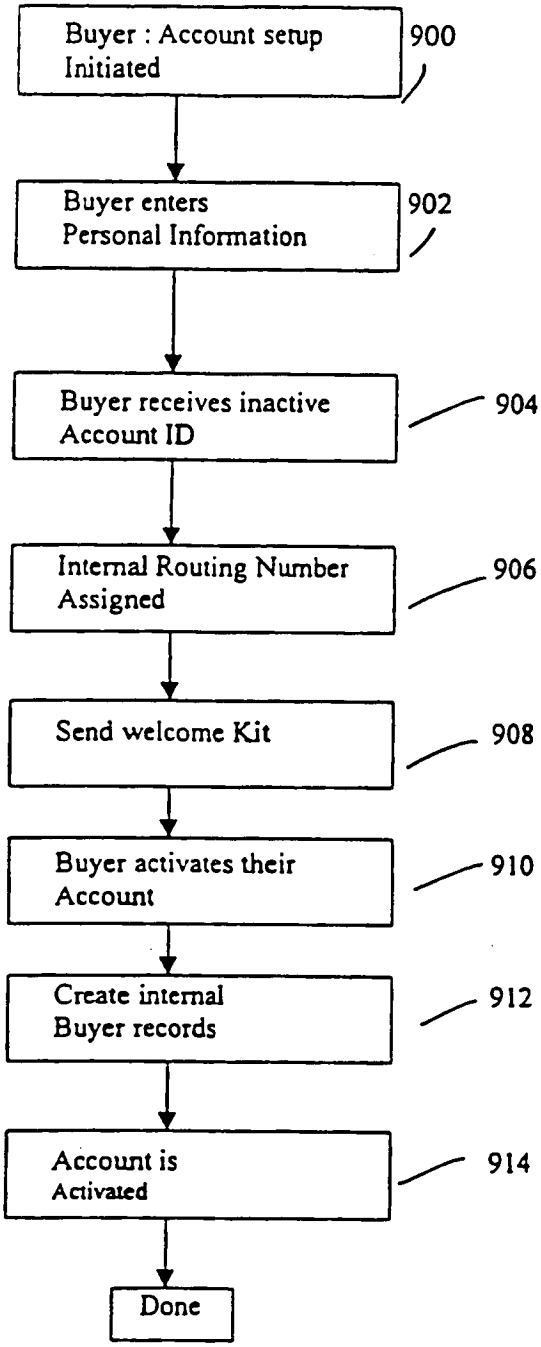


FIGURE 9

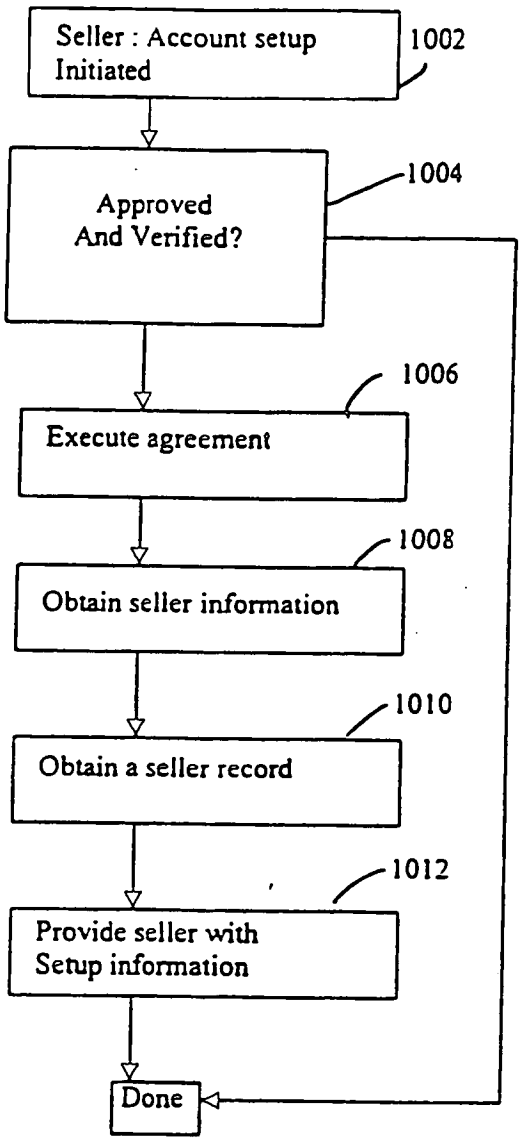


FIGURE 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/15788

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/60
US CL : 705/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/26, 27, 21, 18, 16, 1, 500

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

STN, WEST, EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 6,023,682 A (CHECCHIO) 08 February 2000, abstract, lines 9-12, col. 1, line 66-col. 2, line 25, Fig. 1, col. 2, lines 7-10, col. 3, lines 58-67, col. 4, lines 1-31.	15
---		---
Y,P		1-14,16-27
Y,P	US 6,014,650 A (ZAMPESE) 11 January 2000, abstract, lines 1-2, fig. 3, col. 2, lines 17-22, col. 3, line 14-col. 4, line 13, col. 6, lines 55-56, col. 5, line 59-col. 6, line 7.	1-14, 17, 21, 25-27
Y	US 5,903,721 A (SIXTUS) 11 May 1999, col. 4, lines 6-10	1-27

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 08 SEPTEMBER 2000	Date of mailing of the international search report 03 OCT 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer TOD SWANN Telephone No. (703) 308-1791

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/15788

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,890,137 A (KOREEDA) 30 March 1999, col. 9, lines 5-61	1-27
Y	US 5,825,881 A (COLVIN, Sr.) 20 October 1998, col. 1, line 54-col. 2, line 29, col. 5, lines 14-41, col. 7, lines 17-19, col. 9, lines 16-52, col. 10, line 64-col. 11, line 9, col. 24, lin 48-col. 25, line 8.	5-13
Y	US 5,903,652 A (MITAL) 11 May 1999, figure 1, abstract, lines 15-25.	16, 18-20, 22, 23, 24
Y	US 5,757,917 A (ROSE, et al) 26 May 1998, col. 4, lines 53-65.	19